Configure Wireless Technologies

Track Tagged Assets Using Optimized Monitor Mode on APs

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1 After enabling Monitor mode at the access point level, choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In the Access Points page, click the 802.11 b/g Radio link for the appropriate access point.

Step 3 In the General group box, disable Admin Status by unselecting the check box. This disables the radio.

Step 4 Select the TOMM check box. This check box only appears for Monitor Mode APs. The drop-down lists for each of the four configurable channels are displayed.

Step 5 Choose the four channels on which you want the access point to monitor tags.

Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose None from the channel drop-down list.

Step 6 Click Save. Channel selection is saved.

Step 7 In the Radio parameters page, reenable the radio by selecting the Admin Status check box.

Step 8 Click Save. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM in the Monitor > Access Points page.

Configure Wireless Chokepoints

Creating a Wireless Chokepoint

To add a chokepoint, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Chokepoints.

Step 2 From the Select a command drop-down list, choose Add Chokepoints, and then click Go.

Step 3 Enter the MAC address and name for the chokepoint.

Step 4 Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 5 Enter the coverage range for the chokepoint.

Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 6 Click ok.

After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

Removing a Wireless Chokepoint from the Network

To remove a chokepoint, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Chokepoints.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose Remove Chokepoints, then click Go.

Step 4 Click OK to confirm the deletion.

Manage Unified APs

Configuration

Put APs in Maintenance State

To move an access point to the maintenance state, follow these steps:

Step 1 Click Configuration > Access Points Radio.

The Unified Access Points page appears.

Step 2 In Unified AP Radio tab, select the desired AP(s), and then click Configure > Place in Maintenance State.

The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms are processed with lower severity instead of critical.

Note Reducing the severity of access point down alarms that are in the Maintenance State will not prevent Prime Infrastructure from sending out alarm notification emails, even though the state of the alarm notification policy is "Critical events".

Remove APs from Maintenance State

To remove an access point from the maintenance state, follow these steps:

Step 1 Click Configuration > Access Points Radios.

The Unified AP Radio page appears.

Step 2 In Unified AP Radio tab, select the desired AP(s), and then click Configure > Remove from Maintenance State.

The access points are removed from the maintenance state.

Scheduling

Schedule AP Radio Status Changes

To schedule a radio status change (enable or disable), follow these steps:

Step 1 Click Configuration > Access Points Radios.

Step 2 In Unified AP Radio tab, select the desired APs, and then click Schedule > Schedule Radio Status.

Step 3 Choose Enable or Disable from the Admin Status drop-down list.

Step 4 Use the Hours and Minutes drop-down lists to determine the scheduled time.

Step 5 Click the calendar icon to select the scheduled date for the status change.

Step 6 If the scheduled task is recurring, choose Daily or Weekly as applicable. If the scheduled task is a one-time event, choose No Recurrence.

Step 7 Choose Save to confirm the scheduled task.

View Scheduled AP Radio Status Changes

To view currently scheduled radio status tasks, follow these steps:

Step 1 Click Configuration > Access Points Radios.

Step 2 In Unified AP Radio tab, select the desired APs, and then click Schedule > View Schedule Radio Task(s).

The Scheduled Task(s) information includes:

a. Scheduled Task(s)—Choose the task to view its access points and access point radios.

b. Scheduled Radio admin Status—Indicates the status change (Enable or Disable).

c. Schedule Time—Indicates the time the schedule task occurs.

d. Execution status—Indicates whether or not the task is scheduled.

e. Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.

f. Next Execution—Indicates the time and date of the next task occurrence.

g. Last Execution—Indicates the time and date of the last task occurrence.

h. Unschedule—Click Unschedule to cancel the scheduled task. Click OK to confirm the cancellation.

View Alarms for APs in the Maintenance State

uses critical alarms to track if the managed access points are down. The controller sends three different alarms when the following occurs:

- The Access point is down
- Radio A of the access point is down

- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are grouped into a single alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the Configure > Access Points page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

Configure AP Ethernet Interfaces

To configure an Ethernet interface, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

Note The Access Point Details page displays the list of Ethernet interfaces.

Step 3 Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:

- AP Name—The name of the access point.
- Slot Id—Indicates the slot number.
- Admin Status—Indicates the administration state of the access point.
- CDP State—Select theCDP State check box to enable the CDP state.

Step 4 Click Save.

Configure APs by Importing CSV Files

To import a current access point configuration file, follow these steps:

Note You can use this to configure AP Names, Primary, Secondary, and Tertiary controller details, AP location in bulk.

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Unified AP Radio page, select the applicable AP(s), click Import / Export > Import AP Config.

Step 3 Enter the CSV file path in the text box or click Browse to navigate to the CSV file on your computer.

The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on this page are used for columns not defined in the CSV file.

Sample File Header:

Example:

```
AP Name,Ethernet MAC,Location,Primary Controller,Secondary Controller,Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3
```

The CSV file can contain following fields.

- AP Ethernet MAC Address—Mandatory
- AP Name—Optional
- Location—Optional
- Primary Controller—Optional
- Secondary Controller—Optional
- Tertiary Controller—Optional

Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

- Ethernet MAC—AP Ethernet MAC Address
- AP Name—AP Name
- Location—AP Location
- Primary Controller—Primary Controller Name
- Secondary Controller—Secondary Controller Name
- Tertiary Controller—Tertiary Controller Name

Note Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primary controller and secondary controller entries are empty then a unified access point update is not complete.

Step 4 When the appropriate CSV file path appears in the Select CSV File text box, click OK.

Configure CDP on Access Points

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of the bridge by default.

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 Choose an access point associated with software release 5.0 or later.

Step 3 Click the slots of radio or an Ethernet interface for which you want to enable CDP.

Step 4 Select the CDP State check box to enable CDP on the interface.

Step 5 Click Save.

Manage Autonomous APs

From Prime Infrastructure, the following methods are available for adding autonomous access points

Add Autonomous APs Using Device Information

Autonomous access points can be added to Prime Infrastructure by device information using comma-separated IP addresses and credentials.

Cisco autonomous access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

To add autonomous access points using device information, follow these steps:

Step 1 Click Configuration > Network > Network Devices.

Step 2 Click the Plus icon and select Add Devices from the drop-down menu.

Step 3 In the General tab, enter the IP address of the Cisco Access Point. If you are adding by the DNS name, add the DNS name.

Step 4 On the SNMP tab, choose the SNMP version that you created on Cisco Access Point.

Step 5 If you are using SNMP v1 or v2c, then you must provide the read and write community string that was configured on AP. If you are using SNMP v3, then you must configure:

- Username
- Mode
- Auth.Type
- Auth.Password
- Privacy Type
- Privacy Password

Step 6 On the Telent/SSH tab, configure the Telnet/SSH Parameters.

Step 7 On the HTTP/HTTPs tab, provide HTTPs credentials so that Cisco Prime Infrastructure can collect data from them.

- From the Protocol drop-down list, choose HTTP or HTTPs. The TCP Port will change automatically to the default port for the protocol that you have selected.
- In the TCP Port text box, enter a different TCP Port if you want to override the default.
- Enter the name of a user.
- Enter the password and confirm the same.
- Enter the Monitor username, password, and confirm the password.

Step 8 Click Add.

After the AP is added and its inventory collection is completed, it appears in the Autonomous APs list page (Configuration > Network > Network Devices > Device Type > Autonomous AP. If it is not found in the Autonomous APs list, choose Configuration > Network > Network Devices > Device Type > Unknown Devices page to check the status.

Note Autonomous access points are not counted towards the total device count for your license.

Add Autonomous APs Using CSV Files

Autonomous access points can be added to Prime Infrastructure using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1 Choose Configuration > Network > Network Devices.

Step 2 Click Plus icon and Select Bulk Import option.

Step 3 Click browse to select the applicable CSV file from your system.

Step 4 Click Import.

Bulk Update of Autonomous APs Using CSV Files

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Autonomous AP Radio page, select the checkbox(es) of the desired AP(s).

Step 3 Click Bulk Update APs.
The Bulk Update Autonomous Access Points page appears.

Step 4 Click Choose File to select a CSV file, and then navigate to the CSV file you want to import.

Step 5 Click Update and Sync.

Sample CSV File for Bulk Update of Autonomous APs

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
 snmpv3_auth_password, snmpv3_privacy_type,
 snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,,3,4209.165.201.0,255.255.255.0,v2,public,,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type,
snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,
telnet_timeout209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4209.165.201.0,255.255.255.224,v3,
default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Deleting Autonomous APs from Prime Infrastructure

Note If you replace Autonomous Access Points because of some reason, remove the Autonomous Access Points from Prime Infrastructure before you install the replacement access points on the network.

To remove an autonomous access point from Prime Infrastructure, follow these steps:

Step 1 Select the check boxes of the access points you want to remove. Select the APs that are not associated.

Step 2 Choose Remove APs from the Select a command drop-down list.

View Autonomous APs

Once added, the autonomous access points can be viewed on the Monitor > Access Points page.

Click the autonomous access point to view more detailed information such as the following:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in Monitor > Maps.

They can be added to a floor area by choosing Monitor > Maps floor area and choosing Add Access Points from the Select a command drop-down list.

Download Images to Autonomous APs via TFTP

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or Prime Infrastructure.

To download images to autonomous access points using TFTP, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Autonomous AP Radio tab, select the check box of the autonomous access point to which you want to download an image.

The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 Click Download > Download Autonomous AP Image (TFTP).
The Download images to Autonomous APs page appears.

Step 4 Configure the following parameters:

- File is located on—Choose Local machine or TFTP server.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
- Prime Infrastructure Server Files In—Specify where Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

Step 5 Click Download.

Tip Some TFTP servers might not support files larger than 32 MB.

Download Images to Autonomous APs via FTP

To download images to autonomous access points (using FTP), follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Autonomous AP Radio tab, select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 Click Download > Download Autonomous AP Image (FTP).
The Download images to Autonomous APs page appears.

Step 4 Enter the FTP credentials including username and password.

Step 5 Click Download.

View Autonomous APs in Workgroup Bridge (WGB) Mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as clients in Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all Prime Infrastructure clients that are WGBs, choose Monitor > Clients. From the Show drop-down list, choose WGB Clients, and click Go. The Clients (detected as WGBs) page appears. Click a user to view detailed information regarding a specific WGB and its wired clients.

Note Prime Infrastructure provides WGB client information for the autonomous access point whether or not it is managed by Prime Infrastructure. If the WGB access point is also managed by Prime Infrastructure, Prime Infrastructure provides basic monitoring functions for the access point similar to other autonomous access points.

Export Autonomous AP Details

To export current access point configuration files, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 From the Select a command drop-down list, choose Export AP Config.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

Step 3 Click OK to close the pop-up alert box.

Step 4 Click Go to view the current AP configurations including:

a) AP Name
b) Ethernet MAC
c) Location
d) Primary Controller
e) Secondary Controller
f) Tertiary Controller

Step 5 Select the file option (CSV, Excel, XML) to export the access point configurations.

Step 6 In the File Download window, click Save to save the file.

Configure Access Points XOR Antenna

provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

If you choose Configuration > Wireless echnologies > Access Point Radios, and select an XOR (2.4GHz) or XOR (5GHZ) from the Radio column, the following page appears.

This page contains the following fields:

Note Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Slot ID—Slot ID.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the CDP State check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—From the drop-down choose any of the options: Both Disabled, 5GHz Enabled, 2.4 GHz Enabled, and Both Enabled.

Radio Assignment

- Assignment Method—The assignment methods are: Auto, Serving, or Monitor.

Note Band Selection, RF Channel Assignment, and Tx Power Level Assignment appears only for Serving assignment method.

- Band Selection— You can either choose 2.4 GHz or 5 GHz radio.

Antenna

Depending on the Radio Assignment selection, the following parameters appear:

- Antenna Type—Indicates the antenna type: External or Internal.
- XOR A Antenna—(Displayed only for Auto assignment method). Choose the external antenna or Other from the drop-down list.

- XOR B Antenna—(Displayed only for Auto assignment method). Choose the external antenna or Other from the drop-down list.
- External Antenna—(Displayed for Serving and Monitor assignment method). Choose the external antenna or Other from the drop-down list. The values in the drop-down varies for 2.4 GHz and 5GHz radio.
- Antenna Gain—(Displayed for Serving and Monitor assignment method). Enter the desired antenna gain in the text box. To configure the custom antenna gain, select Others for the External Antenna option.

Note The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear only if you have selected Radio Assignment method as Serving.

- Current Channel—Channel number of the access point.
- Channel Width—Only radios with 20 MHz is supported for a 2.4 GHz radio. For a 5 GHZ radio, from the Channel Width drop-down list, choose 20 MHz, 40 MHz, 80 MHz or 160 MHZ.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the channel of the access point is set globally by the controller.
  - Custom—Use this setting if the channel of the access point is set locally. Select a channel from the Custom drop-down list. The values in the drop-down varies for 2.4 GHz and 5 GHz radios.

11n and 11ac Parameters

- 11n Supported—Indicates whether or not 11n radio is supported.
- 11ac Supported—Indicates whether or not 11ac radio is supported.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

Note The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the power level is set globally by the controller.
  - Custom—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- Antenna A
- Antenna B
- Antenna C
- Antenna D

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose Enable, Disable, or Not Applicable from the drop-down list.

Find Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:

- New Search: Enter an IP address, name, SSID, or MAC, and click Search.
- Saved Searches: Click Saved Search to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

After you click Go, the access point search results appear (see Table 1: Access Point Search Results , on page 15).

Table 1: Access Point Search Results

Field	Options
IP Address	IP address of the access point.
Ethernet MAC	MAC address of the access point.
AP Name	Name assigned to the access point. Click the access point name item to display details.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
AP Type	Access point radio frequency type.
Operational Status	Displays the operational status of the Cisco radios (Up or Down).
Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm
Audit Status	The audit status of the access point.
Serial Number	The serial number of the access point.
AP Mode	Describes the role of the access point modes such as Local, FlexConnect, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect.

Wireless Configuration Groups

Wireless Configuration Groups workflow is the improved workflow of WLAN Controller Configuration Groups feature, which is available in Cisco Prime Infrastructure. With the improved Wireless Configuration workflow, you can:

- Select device specific templates.
- Deploy multiple templates on multiple devices.
- Audit multiple wireless templates from PI.

Note CLI templates and Guest users cannot be deployed from Wireless Configuration Groups.

Create a New Configuration Group

Step 1 Choose Configuration > Wireless Technologies > Wireless Configuration Groups.

Step 2 Click Create to create a new configuration group.
The Configuration Group Workflow wizard appears.

Step 3 In the General Configuration tab, enter the configuration group name, and click Next.
The Select Template tab appears.

Step 4 In the Select Template tab, select the Device Type: CUWN or CUWN-IOS and UA.

Step 5 Drag and drop a template or a group from Templates tree view > My Templates to the Selected Template(s) group box.

The Selected Template(s) group box lists templates or groups, which were added from the Templates tree view.

Step 6 Click Save and Quit to save the configuration group and quit the work flow.

Step 7 Click Next to save the configuration group and to deploy the templates selected.
The Select Devices tab appears.

Step 8 The Select Devices tab lists Controllers based on the device type selected.

Step 9 Select the Device Name check box and click Deploy.
Once the deploy is successful, the Wireless Configuration Groups list page appears.

The Wireless Configuration Groups page contains the following details for the deployed device:

- Group Name
- Last Deployed Devices Count
- Templates Count
- Last Deploy Status
  - Not Initiated —Indicates if the device is deployed on any of the devices or not.
  - Success—Indicates the number of successful templates associated with the applicable IP address.
  - Partial Success / Failure—Indicates the number of failures with provisioning of templates to the applicable controller. Click on Partial Success / Failure link to know the reason for failure.
- Last Undeploy status
- Last Audit Status
- Background Audit—Turn the On/Off toggles to enable the background audit. If this is turned on, then all the templates that are part of this group are audited against the controller during network and controller audits.
- Enforcement—Turn the On/Off toggles to enable the enforcement. If enforcement is turned on, then the templates are automatically applied during the audit if any discrepancies are found.
- Last Modified On
- Last Applied On

Add or Remove Templates from Wireless Configuration Group

The Config Groups Audit page allows you to verify if the controllers configuration complies with the group template. During the audit, you can leave this screen or logout of Cisco Prime Infrastructure. The process continues, and you can return to this page later to view the report.

Note Do not perform any other configuration group functions during the audit verification.

Step 1 Choose Configuration > Wireless Technologies > Wireless Configuration Groups.

Note In Controller List Page, you can click the information icon in Controller List column and then click the export icon to download a CSV file containing details of controllers on which that Configuration Group is configured.

Step 2 Select the Group Name check box, and click Edit.

Step 3 In the Configuration Group Workflow wizard, click Select Templates tab.

Step 4 Choose CUWN or CUWN-IOS.

- Drag and drop a template or a group from the Templates tree view to the Selected Template(s) group box.
- The Selected Template(s) group box will list the selected template or groups which were added from the Templates Tree view.

Step 5 Click Next.

Step 6 In the Device List page, select the devices on which you want to configure the configuration group.

Step 7 Click Deploy to deploy the configuration group on the selected controllers. Or click Save and Quit to configure.

Last Deployed Time column displays timestamp for controllers on which the group is deployed; and displays Not Deployed for the controllers on which the group is only configured.

Audit Wireless Config Groups

The Config Groups Audit page allows you to verify if the controllers configuration complies with the group template. During the audit, you can leave this screen or logout of Cisco Prime Infrastructure. The process continues, and you can return to this page later to view the report.

Note Do not perform any other configuration group functions during the audit verification.

Step 1 Choose Configuration > Wireless Technologies > Wireless Configuration Groups.

Step 2 Select theGroup Name check box, and click Audit.
The Select Devices page appears.

Step 3 Select a Device Name check box and click Audit.

A report is generated and the current configuration on each controller is compared with that in the configuration group template. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

- Audit Status
  - Not Initiated
  - Success—Indicates whether the number of templates associated with the applicable IP address are in sync or not.
  - Not In Sync—Indicates the number of failures with provisioning of templates to the applicable controller. Click Not In Sync to know more details.

View Links in Mesh Networks

You can access mesh link details in several ways:

- Click the Mesh dashboard in home page.
- Choose Monitor > Access Points, click the Mesh Links tab, and click the Details link.
- After you import a KML file from Google Earth, click the AP Mesh link.

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.

- SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.
- Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
- Packet Error Rate Graph—Displays the packet error rates in a graph.
- Link Events—The last five events for the link are displayed.
- Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
- AP Uptime—These statistics help determine if an access point is rebooting frequently.
- LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
- Location Links—Allows you to navigate to Prime Infrastructure map or the Google Earth location.

Define Controller Rogue AP Classification Rules

You can view or edit current rogue access point rules on a single WLC.

To access the rogue access point rules, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose Security > Rogue AP Rules. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

Step 4 Choose a Rogue AP Rule to view or edit its details.

Use Controller Auto-Provisioning to Add and Replace WLCs

simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current Cisco Wireless LAN Controller (WLC). auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note The controller radio and b/g networks are initially disabled by the startup configuration file. You can turn on those radio networks by using a template, which should be included as one of the automated templates.

View the Controller Auto Provisioning List

The Auto Provision Filters page allows you to create and edit auto provisioning filters that define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

For Auto Provisioning privileges, you must have Admin, Root, or Super User status. To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration > User Roles & AAA User Groups > group name > List of Tasks Permitted in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

Filter parameters include:

Parameter	Description
Filter Name	Identifies the name of the filter.
Filter Enable	Indicates whether or not the filter is enabled. Only enabled filters can participate in the Auto Provisioning process.
Monitor Only	If selected, the Cisco WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the Cisco WLC contacts Prime Infrastructure during the auto provisioning process.
Filter Mode	Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).
Config Group Name	Indicates the Configuration Group name. All Config-Groups used by auto provision filters should not have any controller defined in them.

Create Controller Auto Provisioning Filter

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To add an Auto Provisioning Filter:

Step 1 Choose Configuration > Wireless Technologies > WLAN Controller Auto Provisioning.

Step 2 Choose Add Filterfrom the Select a command drop-down list, then click Go.

Step 3 Enter the required parameters.

You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

Step 4 Click Save.

To change the default username and password, you need to delete and then recreate the admin user and explained in Steps 5 through Step 8.

Step 5 To change the default username and password, you need to create a new read/write user on the controller using the Local Management User Template. You must create this new user so that you can delete the default admin user as shown in Step 6.

Step 6 Choose Inventory > Device Manangement > Network Devices, click on the controller name, click the Configuration tab, then select Management > Local Management User, select the admin user, then from the Select a command drop-down list, select Delete Local Management User and click Go.

Step 7 Create a new admin user on the controller using the Local Management User Template.

Step 8 Delete the user you created in Step 5.

Control the Order of Search for Primary Keys Used in Controller Auto Provisioning

Use the Primary Search Key Setting to set the matching criteria search order.

Step 1 Choose Configuration > Plug and Play > Controller Auto Provisioning, then from the left sidebar menu, choose Setting.

Step 2 Click to highlight the applicable search key, then use the Move Up or Move Down buttons to move the search key to a higher or lower priority.

Step 3 Click Save to confirm the changes.

Information About 9800 Series Configuration Model

Cisco Catalyst 9800 Series Wireless Controller simplifies the configuration of the wireless controller using different tags, namely rf-tag, policy-tag, and site-tag. The access points would derive their configuration from the profiles that are contained within the tags.

Profiles are a collection of feature-specific attributes and parameters applied to a specific target. The configuration targets are AP, radio, and WLAN. The rf-tag contains the radio profiles, the policy-tag contains flex-profile and ap-join-profile, and the wireless-tag contains the WLAN profile and policy profile.

The new configuration model (flexconnect mode) helps the central controller to manage sites that are geo-distributed, for example, retail, campus, and so on, where the WLANs are the same. Only, the network and radio profiles have some changes based on the local deployment or topology.

Table 2: Catalyst 9800 Series Configuration Workflow

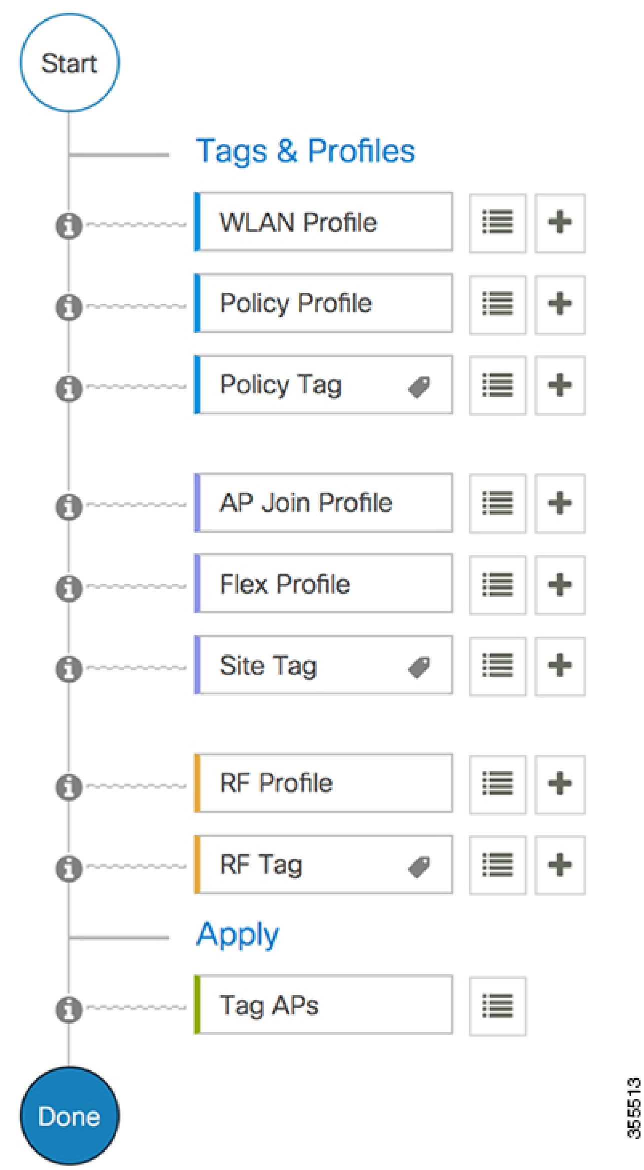
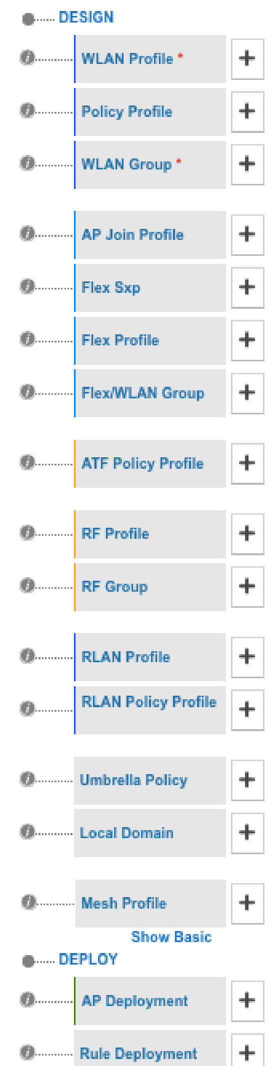
<table>
<tr><th>IOS-XE Polaris</th><th>Prime Infrastructure</th></tr>
<tr><td>
</td>
<td>
</td></tr>
</table>

Table 3: Mapping of UI constructs between IOS-XE Polaris and Prime Infrastructure

IOS-XE Polaris	Prime Infrastructure
Policy Tag	• WLAN Group • Flex WLAN Group (Prime Infrastructure only) Saves mapping of Flex profile and WLAN profile, which is useful in Flex based deployments
RF Tag	RF Profile
Site Tag	AP Deployment and AP Join Profile AP Deployment name is used to create Site tag on device using: • AP Join Profile and Flex-WLAN Group for Flex based deployment • AP Join Profile and WLAN Group for Non-Flex based deployment

Policy Tag

The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client (Quality of Service [QoS] is an exception which constitutes AP policies as well).

The policy tag contains the map of WLAN policy profile. There are 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them is in disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted using the no form of the command in the policy tag.

Site Tag

The site tag defines the properties of a site and contains the flex profile and the AP join profile. The attributes that are specific to the corresponding flex or remote site are part of the flex profile. Apart from the flex profile, the site tag also comprises attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity). For example, the list of primary APs for efficient upgrade is a part of a site tag rather than that of a flex profile.

If a flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and flex profiles are set to default values (default-ap-profile and default-flex-profile).

RF Tag

The RF tag contains the IEEE 802.11a and IEEE 802.11b RF profiles. The default RF tag contains the global configuration. Both these profiles contain the same default values for global RF profiles for the respective radios.

Profiles

Profiles are a collection of feature-specific attributes and parameters applied to a specific target. The configuration targets are AP, radio, and WLAN. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the APs or its associated clients.

WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign different Layer 2 security policies within the same wireless LAN.

To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN definition.

Policy Profile

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for a client that is applied on an AP or controller is moved to the policy profile, for example, VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, BSSID QoS, and so on. However, all the wireless-related security attributes and features on the WLAN are grouped under the WLAN profile.

Flex Profile

Flex profile contains the attributes that are a part of the flex group. However, policy attributes are grouped with the policy profile. The flex profile also contains remote site-specific parameters. For example, the EAP profiles that can be used when the AP acts as an authentication server for local RADIUS server information, VLAN-ACL mapping, VLAN name-to-ID mapping, and so on.

AP Join Profile

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains the following parameters – CAPWAP, IPv4 and IPv6, UDP Lite, High Availability, Retransmit config parameters, Global AP failover, Hyperlocation config parameters, Telnet and SSH, 11u parameters, and so on.

RF Profile

RF profile contains the common radio configuration for the APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings.

Static Association of APs

APs can only be configured statically using the policy-tag, site tag, and RF tag. The APs are identified by the Ethernet MAC address and the association to AP and tag is stored on the controller as a configuration.

Modifying AP Tags

Modifying an AP tag results in DTLS connection reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types, for example, if only policy tag is specified, the default-site-tag and default-rf-tag will be used for site tag and RF tag.

Configure Local Domain for Cisco Umbrella Policy for Cisco Catalyst 9800 Series Wireless Controllers

OpenDNS supports splitting of DNS traffic so that administrator can directly send some desired DNS traffic to intended DNS server (For example, a DNS server located within the Enterprise) thereby, bypassing OpenDNS cloud.

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Local Domain to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 In Regex Pattern area, click the Plus icon to create a new local domain.

Step 4 Enter the URL and Save it.

You need to add this local domain to an Umbrella policy.

Configuring Cisco Umbrella Policy for Cisco Catalyst 9800 Series Wireless Controllers

Cisco Umbrella is a Cloud delivered network security service, which protects devices from malware and breach protection in real time.

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Umbrella Policy to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 Enter or edit the requisite details and select a local domain from the Local Domain dropdown menu.

You need to obtain the token for device from OpenDNS dashboard and ensure it is applied on WLC.

Note Prime Infrastructure 3.5 supports only global policy.

Configure a Flex Sxp Profile for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Flex Sxp to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 Enter or edit the requisite details and Save it.

You need to map this Flex Sxp profile to a Flex profile.

Configure a Flex Profile for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Flex Profile to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 Enter or edit the requisite details.

Step 4 To map a Flex Sxp profile or change it, go to Advanced > General and select the profile from Flex Sxp Profile dropdown menu.

Step 5 Click Save.

Configure Airtime Fairness for Catalyst 9800 Series Wireless Controller

Create Airtime Fairness Policy for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click ATF Policy Profile to view available policies or click the Plus icon to create new. Click an existing ATF policy to edit it.

Step 3 Enter or edit the requisite details.

Step 4 Click Save.

Note You need to map this policy to a Policy Profile.

Add Airtime Fairness Policy to a Policy Profile

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Policy Profile to view available policies or click the Plus icon to create new. Click an existing policy to edit it.

Step 3 Click Access Policies.

Step 4 Under Air Time Fairness Policies, select policy profiles for 2.4 GHz and 5 GHz bands.

You can select separate policies or the same policy for both bands.

Step 5 Click Save.

Enable ATF Policy on an RF profile

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click RF Profile to view available profiles or click the Plus icon to create new. Click an existing profile to edit it.

Step 3 Click Advanced > Air Time Fairness.

Step 4 Select the mode of operation as applicable:

- Disable: To disable ATF on the WLC.
- Enforced: To apply ATF policy on WLC.
- Monitor: To monitor air time usage on your network.

Note You can choose to override the weightage set for WLANs in case of Mesh APs by enabling Override Airtime Allocation. You can enter a weightage for such scenarios when you enable overriding.

Step 5 Click Save.

Configure Remote LAN (RLAN) for Catalyst 9800 Series Wireless Controller

Create RLAN Profile for Cisco Catalyst 9800 Series Wireless Controllers

Remote Lan (RLAN) feature in Prime Infrastructure provides support for wired clients to join the network as wireless clients. WLC authenticates the wired clients. Once a wired client successfully joins, the LAN ports can switch the traffic in Central switching mode or local switching mode depending on the configuration.

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click RLAN Profile to view available policies or click the Plus icon to create new. Click an existing policy to edit it.

Step 3 Enter or edit the requisite details and click Save.

Note You need to map this profile to a WLAN Group.

Create RLAN Policy Profile for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click RLAN Policy Profile to view available policies or click the Plus icon to create new. Click an existing policy to edit it.

Step 3 Enter or edit the requisite details and click Save.

You can also configure Access Policies, QoS and AVC, and Advanced parameters.

Note You need to map this profile to a WLAN Group.

Configure WLAN Group for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click WLAN Group to view available groups, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 In WLAN Mapping tab, select the WLAN profile(s) and the policy profile you want to map them to.

Step 4 Click Map To Policy.

Step 5 In RLAN Mapping tab, select the ports on which you want to activate the profile.

Note Ensure these ports are enabled on the AP.

Lightweight Access Points > AP Parameters > AP LAN Port configuration.

Deploy a Rule On Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Rule Deployment to view available policies or click the Plus icon to create a new. Click an existing rule to edit it.

Step 3 Enter the requisite details for the following fields:

- Rule Name – Enter he name of the deployment rule

- AP Name Contains – Enter a regular expression (regex) on the basis of which you want to select the APs on which this rule is deployed.
- Deployment Mode – Select the deployment mode (Flex based or Non-Flex based.

Step 4 Select the Flex Profile, WLAN Group, AP Join Profile, and RF Group from their respective drop-down menus.

Step 5 Click Save.

Step 6 Cick Rule Deployment again to view the list of available rules.

Step 7 Select the rule(s) you want to deploy and then click Deploy.

Step 8 Choose from the available deployment options and then click Deploy.

To see the rule(s) deployed on your Catalyst 9800 Series Wireless Controller, click Configuration > Network > Network Devices > Device Groups > Device Type > Cisco Catalyst 9800 Series Wireless Controller for Cloud > . Click on your Catalyst 9800 Series device and then click Configuration > System > Rule Deployment.

Translate Cisco AireOS Controller Configurations to Cisco Catalyst 9800 Series Controller

AireOS Config Translator provides you with a seamless migration from a legacy Cisco WLC to a Cisco Catalyst 9800 Series Wireless Controller.

Note

- This feature works with Cisco WLCs running AireOS versions 8.8 and above.
- The conversion process may take longer if the WLC configuration is greater than 5000CLIs.
- When you translate an AireOS configuration using AireOS Config Translator, if there are WLANs which have the same IDs as the ones already on the Catalyst 9800 Controller, they are not created.

Before you begin

Please ensure the following criteria are met:

- Both the legacy (AireOS) WLC and the Catalyst 9800 Series controller should already be managed in Prime Infrastructure.
- Both the devices (AireOS and Catalyst 9800 Series) should be added to Prime Infrastructure with valid SNMP and CLI credentials.

Step 1 Click Configuration > Wireless Technologies > AireOS Config Translator.

Step 2 Select the AireOS device from the Select a source AireOS Device list on the Choose Source page.

Step 3 Select the appropriate Catalyst 9800 Series Controller from Select a Target 9800 Device list.

Step 4 Click Fetch Config.

This obtains the Running Config from the source WLC.

Step 5 Click Translate on the Verify and Update Config page.

This translates the fetched AireOS configurations to their Catalyst 9800 Series counterparts. The translated configurations get categorized as follows:

a. Supported – CLIs which were successfully translated

b. Unsupported – CLIs which are either not supported or did not get translated

c. Not Applicable – CLIs for which no translation is required

Step 6 Modify the hostname, passwords, and pre-shared keys in the Supported configurations (highlighted).

Step 7 Check the Accept to deploy checkbox.

Step 8 Click Deploy.

Step 9 Select the APs that you want to migrate and then click Migrate.

Results:

- The primary controller's name and IP address are configured.
- Sync is automatically triggered on Prime Infrastructure.

Related Topics

Add Devices to